

Електронний журнал «Ефективна економіка» включено до переліку наукових фахових видань України з питань економіки (Категорія «Б», Наказ Міністерства освіти і науки України № 975 від 11.07.2019). Спеціальності – 051, 071, 072, 073, 075, 076, 292.
Ефективна економіка. 2022. № 11.

DOI: <http://doi.org/10.32702/2307-2105.2022.11.20>

УДК 681.3

В. І. Чубаєвський,

к. політ. н., доцент, доцент кафедри інженерії програмного забезпечення та кібербезпеки, Державний торговельно-економічний університет
ORCID ID: <https://orcid.org/0000-0001-8078-2652>

МЕТОДИЧНИЙ ПІДХІД ДО ОЦІНКИ ЕКОНОМІЧНОЇ ЕФЕКТИВНОСТІ СИСТЕМИ ЗАХИСТУ КОРПОРАТИВНОЇ ІНФОРМАЦІЇ

V. Chubaievskyi,

*PhD in Political Sciences, Associate Professor, Associate Professor of the
Department of Engineering of software and cyber security, State University of
Trade and Economics*

METHODOLOGICAL APPROACH TO ASSESSING THE ECONOMIC EFFICIENCY OF THE CORPORATE INFORMATION SECURITY SYSTEM

У статті науково обґрунтовано та доведено, що економічний підхід до оцінки ефективності системи захисту корпоративної інформації та вибору корпоративної інформаційної політики на базі цієї оцінки дозволяє оптимізувати стану системи захисту корпоративної інформації відповідно до умов функціонування на рівні конкретної корпоративної структури.

Проведені дослідження дозволили запропонувати методичний підхід до оцінки економічної ефективності системи захисту корпоративної інформації, який, на відміну від наявних, передбачає здійснення оцінювання ступеня досягнення максимально можливого прибутку корпоративної структур за рахунок визначення потенційних можливостей системи захисту корпоративної інформації, який сприяє отриманню своєчасної та достовірної інформації як основи для прийняття та реалізації суб'єктами безпеки тактичних і стратегічних управлінських рішень та дозволяє надавати керівникам корпорацій комплексну оцінку ефективності управлінських дій щодо використання інноваційних технологій інформаційної безпеки на усіх ієрархічних рівнях організаційної структури управління.

The article scientifically substantiates and proves that the economic approach to assessing the effectiveness of the corporate information security system and the choice of corporate information policy based on this assessment allows to optimize the state of the corporate information security system in accordance with the conditions of functioning at the level of a particular corporate structure. The approach to assessing the economic efficiency of the corporate information protection system based on the economic criterion of the progressiveness of the corporate information system creates the prerequisites for determining its optimal state.

Progressive (effective) are the following elements of the corporate information protection system, forms and methods of organization and management of corporations, with the help of which it is possible to ensure the implementation of the specified results with minimal total costs of living and urethral labor with mandatory compliance with the standards of social and environmental responsibility of corporate structures.

The conducted research allowed us to propose a methodical approach to assessing the economic efficiency of the corporate information security system, which, unlike the existing ones, provides for the assessment of the degree of

achievement of the maximum possible profit of corporate structures by determining the potential capabilities of the corporate information security system, which contributes to obtaining timely and reliable information as a basis for the adoption and implementation of tactical and strategic management decisions by security entities and allows to provide

The implementation of a methodological approach to assessing the economic efficiency of the corporate information security system based on determining the degree of its progress will allow to assess the current state of the corporate information security system and to form a vector for achieving its optimal (best) variant in the specific conditions of functioning of corporations for permanent monitoring of the achievement of goals and objectives of the information security system and determining the directions of necessary changes.

Ключові слова: *інформаційні ресурси та технології; інформаційна система; корпорація; корпоративна інформація; система захисту корпоративної інформації; економічна ефективність.*

Keywords: *information resources and technologies; information system; corporation; corporate information; corporate information security system; economic efficiency.*

Постановка проблеми. У діяльності сучасних корпоративних структур використовується велика кількість різних методик оцінки економічної ефективності системи захисту корпоративної інформації, які зазвичай називають методиками оцінки рівня інформаційної безпеки. Ці методики передбачають чи поодинокі показники, чи його набори, за допомогою яких робляться спроби кількісно оцінити стан системи захисту корпоративної інформації. Проте, існуючи методики не дають можливість оцінити стан системи захисту корпоративної інформації та її економічну ефективність з погляду їх можливостей реалізації цілей діяльності корпоративних структур,

тобто з погляду ресурсного підходу та врахувати особливості життєвого циклу корпоративної інформації.

Відсутність поки що єдиної методики чи рекомендацій, регламентуючих універсальні для всіх галузей національної економіки принципи визначення економічної ефективності системи захисту корпоративної інформації ускладнює роботу зі створення надійних методів вимірювання ступеня досконалості та прогресивності інформаційної системи.

Аналіз останніх досліджень і публікацій. Питання формування методики оцінки економічної ефективності системи захисту корпоративної інформації досліджували такі вітчизняні та зарубіжні вчені як: З.Валіулліна [4], В. О.В. Гордієнко [5], В. Домарєв [5], А. Страхарчука [7], О. Черевко [8], С. Парк [9], Т. Руїджхавер [9], К.С. Хонг [10] та інші.

Однак, слід зазначити, що головним недоліком для більшості застосовуваних методів оцінки економічної ефективності системи захисту корпоративної інформації є відсутність економічного змісту у показниках оцінки, що використовуються. Зазвичай застосовують показники, що мають умовний характер. Такий підхід не дозволяє простежити економічні наслідки зміни корпоративної інформаційної системи та швидко здійснювати трансформацію її елементів в залежності від конкретних умов функціонування корпорацій.

Метою статті є обґрунтування необхідності та подальшого розвитку методичного підходу до оцінки економічної ефективності системи захисту корпоративної інформації, що буде сприяти проведенню комплексної оцінки ефективності управлінських дій щодо використання інноваційних технологій інформаційної безпеки на усіх ієрархічних рівнях організаційної структури управління.

Виклад основного матеріалу дослідження. Показники системи захисту корпоративної інформації дуже складно взаємопов'язані з економічними показниками і не завжди заздалегідь можна визначити, в який бік та наскільки їх слід змінювати. Елементи інформаційної системи

корпорації традиційно віднесене до групи прогресивних ресурсів, незважаючи на їх високі технічні характеристики, у конкретних умовах функціонування корпорацій може виявитися неефективним з економічної точки зору [1, с.23].

Отже, розробка корпоративної політики щодо впровадження ефективної системи захисту корпоративної інформації з урахуванням цієї оцінки орієнтує на «максимізацію» рівня системи захисту корпоративної інформації та у деяких випадках може призвести до великого спотворення відповідності цієї системи умовам функціонування корпоративних структур.

Одним з підходів, що дозволяють виявити і звести зазначений розрив (невідповідність) до мінімуму на основі визначення стану системи захисту корпоративної інформації, що повністю відображає умови функціонування корпоративних структур, є економічний підхід до оцінки ефективності системи захисту корпоративної інформації.

Концепція економічної оцінки системи захисту корпоративної інформації виходить з принципу - рівень системи захисту корпоративної інформації є передумовою, умовою його ефективності [2, с.21]. Високий рівень системи захисту корпоративної інформації – високі економічні показники функціонування корпорацій. Прогресивними (ефективними) є такі елементи системи захисту корпоративної інформації, форми та методи організації та управління діяльністю корпорацій, за допомогою яких можна забезпечити виконання заданих результатів з мінімальними сукупними витратами живої та уречевленої праці за обов'язкового дотримання нормативів соціальних та екологічних відповідальності корпоративних структур.

В основу економічного підходу до оцінки системи захисту корпоративної інформації та вибору корпоративної інформаційної політики на базі цієї оцінки закладено принцип оптимізації стану системи захисту корпоративної інформації за умовами функціонування на рівні конкретної корпорації. Ступінь відхилення від цього оптимального стану визначає

рівень ефективності системи захисту корпоративної інформації. Чим вище рівень системи захисту корпоративної інформації, тим ближчий фактичний стан до оптимального.

Таким чином, підхід до оцінки економічної ефективності системи захисту корпоративної інформації на основі економічного критерію прогресивності інформаційної системи корпорацій створює передумови визначення її оптимального стану. На рис. 1 показано реалізацію аналізованого підходу на базі визначення областей економічно ефективного використання інформаційних ресурсів і технологій.

Так, у заштриховану область E множини $A(E \subset A)$, сукупністю елементів якого визначається стан системи захисту корпоративної інформації, потрапляють ті елементи інформаційної системи, які за умов діяльності корпорації, що визначаються елементами множини $K(K \subset B)$ є непрогресивними. При цьому до розряду непрогресивних слід віднести:

1. Елементи інформаційної системи, потенційні можливості яких не можуть бути реалізовані ефективно за умов функціонування корпорацій.

ΔP^1 - пов'язані із цим зайві витрати (рис. 1, б).

2. Елементи інформаційної системи корпорацій, замість яких можуть бути поставлені відповідно до умов функціонування корпорацій, що склалися, на які слід замінити наявну по причині її ширших функціональних можливостей. ΔP^2 - витрати, пов'язані з зазначеною невідповідністю (рис. 1, в).

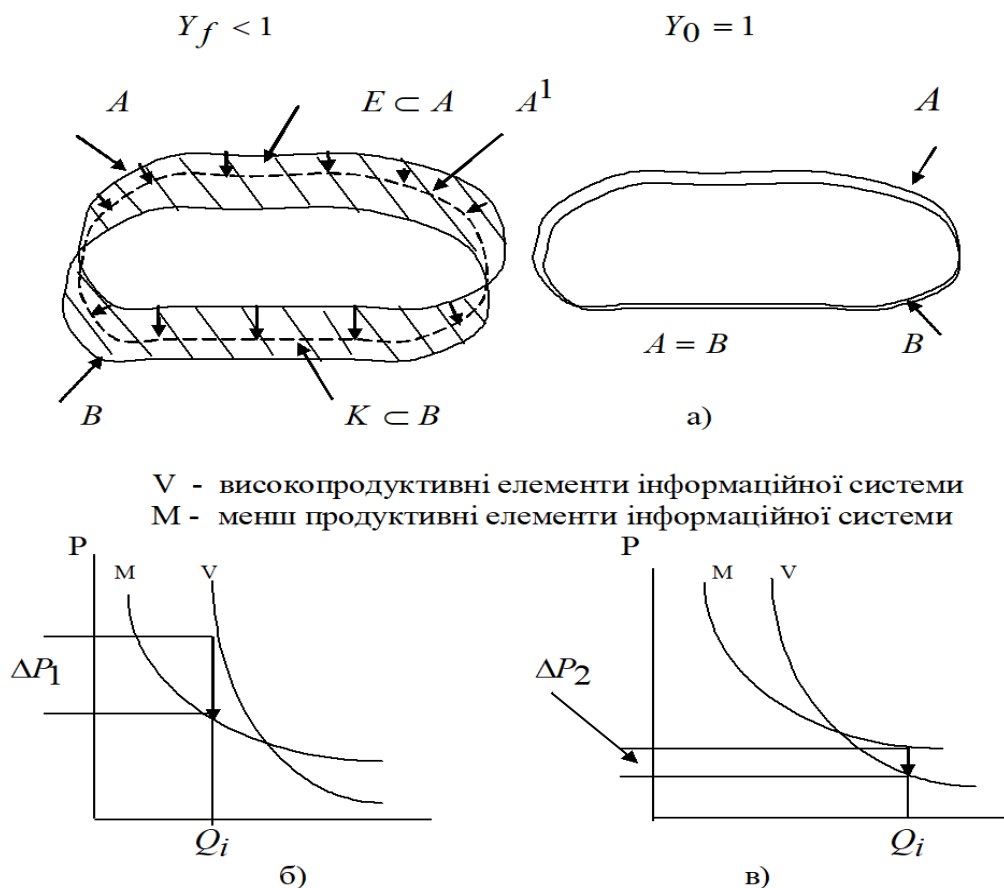


Рис. 1. Области ефективного використання інформаційної системи
Джерело: розроблено автором

Як параметр, що визначає умови функціонування корпорацій, прийнятий заданий обсяг подолань загроз та ризиків інформаційної безпеки корпорацій $Q_i \in B$ за певний період; P - питомі витрати, пов'язані з використанням взаємозамінних елементів інформаційної системи корпорації.

Таке розмежування дозволяє розкривати конкретні шляхи ($A \rightarrow A^1$) та засоби підвищення рівня системи захисту корпоративної інформації. Співвідношення між $A \cap B$ і B характеризує ступінь поширення у діяльності корпорацій прогресивних засобів і методів, що належать області $A \cap B$, в загальній їх кількості в корпорації (B).

$A=B$ - оптимальний стан, при якому існуюча система захисту корпоративної інформації повністю відповідає об'єктивно сформованим умовам функціонування корпорацій.

Y - показник кількісної оцінки ступеня близькості фактичного стану існуючої системи захисту корпоративної інформації до оптимального.

Таким чином, економічна ефективність системи захисту корпоративної інформації кількісно оцінюється ступенем відхилення фактичних річних приведених витрат (P_f), пов'язаних з існуючою системою захисту корпоративної інформації від рівня витрат, що відповідає оптимальному її стану (P_o).

$$Y = 1 - \frac{P_f - P_o}{P_f} \quad (1)$$

при цьому: $Y_o = 1$ - оптимальне значення;

$0 \leq Y_f \leq 1$ - фактичне значення.

Графічна інтерпретація показника Y наведено на рис. 2.

Такий підхід до оцінки економічної ефективності системи захисту корпоративної інформації є доцільним при централізованому розподілі інвестицій та ресурсів корпорацій [3, с.136].

Враховуючи динамічність сучасного бізнес-середовища корпорацій показник економічної ефективності системи захисту корпоративної інформації має визначатися як рівень досягнення нормативу потенційної можливості системи захисту корпоративної інформації.

За наявності таких нормативів рівень потенційних можливостей системи захисту корпоративної інформації Y_{ib} може бути оцінений економічно як ступінь досягнення максимально можливого прибутку корпоративної структури:

$$Y_{ib} = 1 - \frac{D_n - D_f}{D_n} \quad (2)$$

де

D_n - прибуток, який може бути отриманий в умовах функціонування корпорації, що відповідають нормативу потенційної спроможності системи захисту корпоративної інформації;

D_f - прибуток, який отримує корпорація при фактично досягнутих умовах функціонування системи захисту корпоративної інформації.

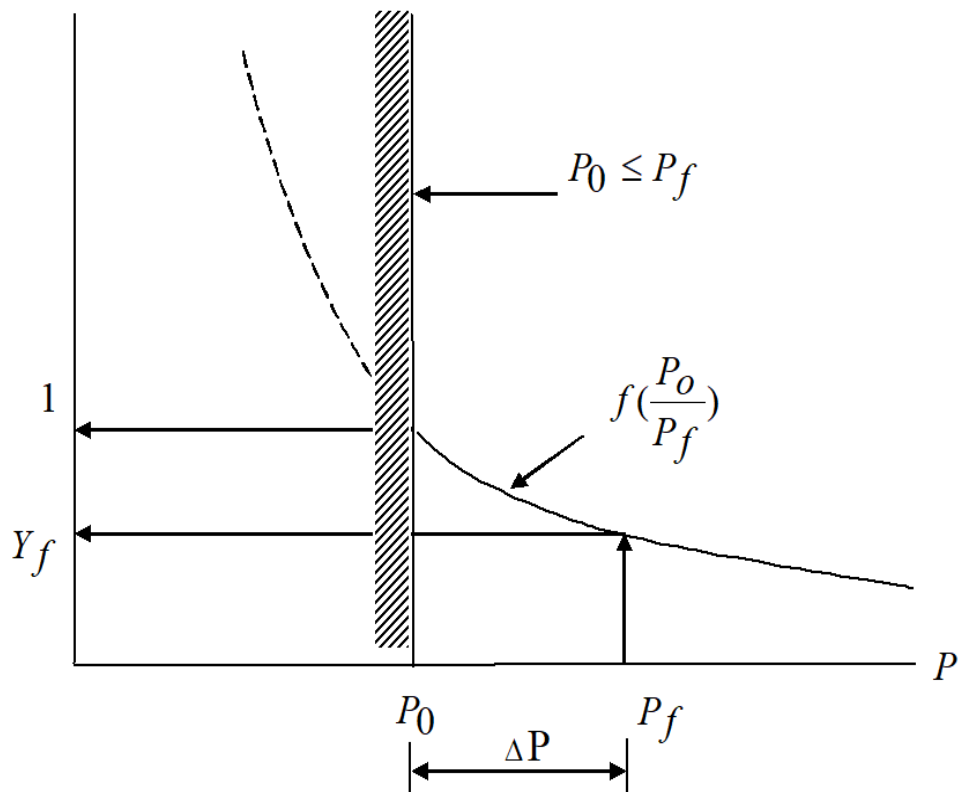


Рис.2. Графічна інтерпретація показника економічної ефективності системи захисту корпоративної інформації

Джерело: розроблено автором

Значення D_n визначається економічною службою підприємства за роками запланованого періоду з урахуванням результатів реалізації цільової комплексної програми впровадження системи захисту корпоративної інформації. При цьому розраховують величину прибутку, який може бути отриманий у тому чи іншому році планового періоду. Якщо за конкретними умовами функціонування неможливо ефективно використати систему захисту корпоративної інформації, встановлюється норматив частки коштів, що використовуються в економічно підрозділах корпорації від загального обсягу всієї інформаційної системи. Ця частка приймається як норматив потенційної можливості системи захисту корпоративної інформації на запланований рік. Значення визначають із фінансового звіту підприємства щодо кожного року аналізованого періоду.

Приведення системи захисту корпоративної інформації у відповідність з умовами функціонування підприємства, що постійно змінюються, визначає динамічність завдання, необхідність розгляду її в постійному розвитку.

Отже, економічний підхід до оцінки прогресивності системи захисту корпоративної інформації дозволяє не тільки оцінити існуючий стан (A), але і націлює на вибір і досягнення оптимального (найкращого) її стану ($A \rightarrow A^1 \rightarrow B$) в конкретних умовах функціонування корпорацій.

Внаслідок високого рівня мінливості умов функціонування корпорацій за порівняльної стійкості їх інформаційних систем об'єктивно існує процес постійної розбіжності фактичного значення економічної ефективності системи захисту корпоративної інформації від його досягнутого оптимального рівня. Отже, вирішення цього завдання передбачає кількісну оцінку факторів, що визначають рівень інформаційної безпеки, їхнього безпосереднього впливу та зв'язку з ефективністю функціонування корпорацій.

Оцінка швидкості реагування на зміни у зовнішньому середовищі характеризує властивість ефективної системи захисту корпоративної інформації забезпечувати адаптивність корпоративних структур від зовнішніх та внутрішніх загроз. Наявність виявлених проблем доводить необхідність розробки методики оцінки економічної ефективності системи захисту корпоративної інформації.

Об'єктом оцінки є 250 вітчизняні підприємств з чисельністю працівників понад 250 осіб, до складу яких входять підрозділи чи служби інформаційної безпеки. Діагностика проблем оцінки економічної ефективності системи захисту корпоративної інформації проводилася методом діагностичного інтерв'ю. Інтерв'ю проводилося з керівниками підприємств та керівникам служб (департаментів) інформаційної безпеки з метою отримання відповідей на дослідницькі питання:

- Чи є проблема оцінки ефективності та релевантна існуюча система

захисту корпоративної інформації?

- Чи існує на підприємстві локальний нормативний акт, який регулює систему захисту корпоративної інформації та визначає методику оцінки її ефективності?

- Як часто на Вашому підприємстві здійснюється оцінка ефективності системи захисту корпоративної інформації?

- Які цілі оцінки економічної ефективності системи захисту корпоративної інформації?

- Які методології та індикатори використовуються для

- Оцінки економічної ефективності системи захисту корпоративної інформації?

- Які проблеми оцінки економічної ефективності системи захисту корпоративної інформації виникають на Вашому підприємстві?

- Який із підходів, запропонованих у науковій літературі для оцінки економічної ефективності системи захисту корпоративної інформації є найкращім?

Керівники підприємств та керівники служб (департаментів) інформаційної безпеки великих та середніх підприємств вказують на актуальність оцінки економічної ефективності системи захисту корпоративної інформації. Однак вони не виділяють чітко відмінних рис оцінки ефективності цих систем. Крім того, на більшості досліджуваних підприємств взагалі відсутні методики оцінки економічної ефективності системи захисту корпоративної інформації, в окремих випадках локальними нормативними актами визначається склад узагальнюючих показників оцінки ефективності. тому, основні висновки ґрунтуються на суб'єктивних оцінках.

Однак, практично на всіх підприємствах для оцінки економічної ефективності системи захисту корпоративної інформації розраховуються такі показники, як: витрати на забезпечення системи захисту корпоративної інформації, рівень виконання бюджету видатків департаменту інформаційної безпеки, розмір попереджуючої, виявленої та відшкодованої шкоди.

У цілому, слід зазначити, що керівники не вважають оптимальними підходи, що використовуються для оцінки економічної ефективності системи захисту корпоративної інформації, та вказують на недостатню теоретичну та методологічну опрацьованість даного напрямку.

Проведене дослідження дозволило виявити та систематизувати проблеми оцінки економічної ефективності системи захисту корпоративної інформації на підприємствах:

- недостатня розробленість методики оцінки рівня інформаційної безпеки підприємства, адаптованої до цілей оцінки ефективності та ефективності системи захисту корпоративної інформації;

- існуючі методики оцінки рівня інформаційної безпеки підприємства не враховують витрати ресурсів, що спрямовуються на функціонування системи захисту корпоративної інформації;

- недостатня розробленість методики оцінки попередженого збитку, який є результатом посилення захисту економічних інтересів та інформаційного потенціалу підприємства від зовнішніх загроз. Високий рівень суб'єктивності результатів оцінювання;

- це орієнтує працівників служби економічної безпеки на блокування більшості управлінських рішень, пов'язаних з ризиком, що негативно позначається на швидкості прийняття управлінських рішень і результатах діяльності підприємства;

- існуючі системи захисту корпоративної інформації не враховують ефект від заходів, спрямованих на підвищення безпеки від внутрішніх загроз.

Оцінка ефективності та результативності системи захисту корпоративної інформації повинна здійснюватися керівництвом підприємства з метою контролю за досягненням цілей та завдань функціонування інформаційної безпеки та визначення напрямків необхідних змін [4, с.11].

Методика оцінки ефективності та економічності системи захисту корпоративної інформації базується на дотриманні низці принципів [5, с.38]:

- комплексності – облік кінцевих та безпосередніх результатів функціонування системи захисту корпоративної інформації;
- з урахуванням стадії розвитку корпоративних систем та життєвого циклу корпоративної інформації;
- об'єктивності – виключення суб'єктивних чинників, які впливають на результати оцінки;
- рентабельності – витрати ресурсів на оцінку повинні бути меншими за отриманий ефект;
- цифровізації – використання процедур та інформаційних технологій для збирання та обробки даних у процесі оцінки економічної ефективності системи захисту корпоративної інформації.

Кінцевим результатом функціонування системи захисту корпоративної інформації є забезпечення захищеності економічних інтересів корпоративних структур від зовнішніх та внутрішніх загроз у короткостроковій та довгостроковій перспективі. Досягнення кінцевого результату вимагає реалізації комплексу процесів розробки, прийняття та реалізації управлінських рішень, що мають різну тривалість та заплановані терміни реалізації [6, с.103]. Для того, щоб спрогнозувати кінцевий результат і виявити потенційні ризики недосягнення цілей у довгостроковій перспективі, необхідно оцінити безпосередні результати функціонування системи захисту корпоративної інформації – результати процесів, вкладених у досягнення цільового рівня економічної ефективності інформаційної безпеки..

Оцінка ефективності системи захисту корпоративної інформації включає порівняння рівня продуктивності з рівнем виконання бюджету щодо створення такої системи.

Запропонований підхід до оцінки ефективності виходить із того, що бюджет витрат на експлуатацію системи захисту корпоративної інформації виправданий і дозволяє повністю фінансувати заплановані заходи щодо забезпечення інформаційної безпеки корпорацій

Інформаційною базою для оцінки економічної ефективності системи

захисту корпоративної інформації виступили дані 250 українських підприємств, зокрема:

- дані внутрішнього управлінського обліку;
- стратегічний та оперативний плани підприємства, звіти про виконання планів;
- граничні значення показників системи захисту корпоративної інформації підприємств;
- плани забезпечення інформаційної безпеки підприємства та звіти про їх виконання;
- результати ревізій, результати судово-економічних експертиз та інші достовірні джерела інформації.

Отже, оцінка економічної ефективності системи захисту корпоративної інформації здійснюється з метою моніторингу досягнення цілей і завдань функціонування системи інформаційної безпеки та визначення напрямів необхідних змін.

Кінцевим результатом оцінювання результативності та результативності є формування адекватних заходів, спрямованих на виявлення та усунення проблем функціонування системи захисту корпоративної інформації, зменшення негативного впливу викликів і загроз інформаційної безпеці підприємства, попередження або мінімізацію можливих збитків.

Реалізація зазначених завдань оцінки економічної ефективності системи захисту корпоративної інформації з урахуванням економічного підходу є найважливішим елементом постійно діючого механізму управління розвитком корпоративних структур.

Висновки. Оцінювання економічної ефективності системи захисту корпоративної інформації дозволило визначити ступінь досягнення максимально можливого прибутку корпоративними структурами та розробити рейтингову шкалу оцінки ефективності системи захисту корпоративної інформації, посилити управлінські заходи у процесі

формування стратегії та механізмів забезпечення комплексної системи корпоративної інформаційної безпеки при формування адекватних заходів, спрямованих на виявлення та усунення проблем функціонування системи захисту корпоративної інформації, зменшення негативного впливу викликів і загроз інформаційної безпеці, попередження або мінімізацію можливих збитків.

Література

1. Бакай В. Й., Зима В. М. Нові виклики та особливості створення системи інформаційної безпеки підприємства. *Вісник Хмельницького національного університету*. 2020, № 5. С.19-22.
2. Бодюл Є. М. Інформаційна безпека банку. Протидія злочинам, які вчиняються з використанням комп'ютерних мереж: тези доповідей Міжнародної науково-практичної конференції (м. Севастополь, 1–2 жовтня 2010 року). Державний вищий навчальний заклад «Українська академія банківської справи Національного банку України». Суми : ДВНЗ «УАБС НБУ», 2010. С.135-137.
3. Бондаренко М. Ф., Потій О. В., Горбенко Ю. І. та ін. Визначення та обґрунтування суті політики інформаційної безпеки. *Радиотехника*. 2003. № 134. С. 9-25.
4. Валіулліна З. В. Інформаційна безпека корпоративної економіки в умовах глобалізаційних процесів. *Вісник Дніпропетровського університету*. Серія : Менеджмент інновацій. 2016. Випуск 6. С.34-41.
5. Домарєв В. В., Гордієнко О.В. Обґрунтування основних функцій системи управління інформаційною безпекою. *Вісник Державного університету інформаційно-комунікаційних технологій*. 2012. Т. 10, № 2. С. 102-104.
6. Жабинець О. Й. Політика інформаційної безпеки страхових компаній: українські реалії та досвід США. *Проблеми економіки*. № 4. 2014. С.22-27
7. Страхарчук А. Я., Страхарчук В. П. Інформаційні системи і технології в банках: Навч. посіб. К.: УБС НБУ: Знання, 2010. 515 с.

8. Черевко О.В. Теоретичні засади поняття інформаційної безпеки та класифікація загроз системі інформаційного захисту. *Ефективна економіка*. № 5, 2014. URL: <http://www.economy.nayka.com.ua/?op=1&z=3304> (дата звернення: 3.01.2022)
9. Park, S., and Ruighaver, T. (2008). "Strategic Approach to Information Security in Organizations," ICISS. International Conference on Information Science and Security, 2008: IEEE, pp. 26-31
10. Hong, K.-S., Chi, Y.-P., Chao, L., and Tang, J.-H. (2003). "An Integrated System Theory of Information Security Management," *Information Management & Computer Security* (11:5), pp 243-248. [in English].
11. Kim, S.H., Wang, Q.-H., and Ullrich, J.B. (2012). "A Comparative Study of Cyberattacks," *Communications of the ACM* (55:3), p 66. [in English].
12. Soomro, Z.A., Shah, M.H. and Ahmed, J. (2016), "Information security management needs more holistic approach: a literature review", *International Journal of Information Management*, Vol. 36 No. 2, pp. 215-225, doi: 10.1016/j.ijinfomgt.2015.11.009.

References

1. Bakai, V. Y. and Zyma, V. M. (2020), "New challenges and features of creating an information security system of the enterprise", *Bulletin of Khmelnytsky National University*, vol. 5, pp.19-22.
2. Bodiul, Ye. M. (2010), Information security bank *Informatsiina bezpeka banku: protydiia zlochynam, yaki vchyniaiutsia z vykorystanniam kompiuternykh merezh*. [Information security of the bank. Combating crimes committed with the use of computer networks. Abstracts of reports of the International scientific-practical conference (Sevastopol, October 1-2, 2010)], State Higher Educational Institution "Ukrainian Academy of Banking of the National Bank of Ukraine". SHEI "UABS NBU", Sumy, Ukraine, pp.135-137.
3. Bondarenko, M. F., Potii, O. V. and Horbenko, Yu. I. (2003), "Definition and substantiation of the essence of information security policy", *Radio engineering*, Vol. 134, pp. 9-25.

4. Valiullina, Z. V. (2016), "Information security of the corporate economy in the context of globalization processes", *Bulletin of Dnipropetrovsk University. Series: Innovation Management*, vol. 6, pp.34-41.
5. Domariiev, V. V. and Hordiienko, O.V. (2012), "Substantiation of the main functions of the information security management system", *Bulletin of the State University of Information and Communication Technologies*, vol. 10, no. 2, pp. 102-104.
6. Zhabynets, O. Y. (2014), "Information security policy of insurance companies: Ukrainian realities and USA experience", *Problems of economics*, vol. 4, pp.22-27.
7. Strakharchuk, A. Ja. and Strakharchuk, V. P. (2010), *Informacijni systemy i tekhnologhiji v bankakh*. [Information systems and technologies in banks], UBS NBU: Knowledge, Kyiv, Ukraine.
8. Cherevko, O.V. (2014), "Theoretical foundations of the concept of information security and classification of threats to the information security system", *Effective Economy*, vol. 5, available at: <http://www.economy.nayka.com.ua/?op=1&z=3304> accessed: 17 December 2021).
9. Park, S., and Ruighaver, T. (2008), "Strategic Approach to Information Security in Organizations," ICISS. International Conference on Information Science and Security, IEEE, pp. 26-31.
10. Hong, K.-S., Chi, Y.-P., Chao, L., and Tang, J.-H. (2003), "An Integrated System Theory of Information Security Management", *Information Management & Computer Security*, vol. (11:5), pp 243-248.
11. Kim, S.H., Wang, Q.-H., and Ullrich, J.B. (2012), "A Comparative Study of Cyberattacks", *Communications of the ACM*, vol. (55:3), p 66.
12. Soomro, Z.A., Shah, M.H. and Ahmed, J. (2016), "Information security management needs more holistic approach: a literature review", *International Journal of Information Management*, Vol. 36, No. 2, pp. 215-225, doi: 10.1016/j.ijinfomgt.2015.11.009.

Стаття надійшла до редакції 02.11.2022 р.